WHAT IS CLAIMED IS:

1. A method of responding to an intrusion, the method comprising:

selectively responding to at least one notification of an intrusion, from a network-accessible intrusion detection service (IDS) manager, by a computer evaluating the notification based on local IDS policy that includes information relating to the notification of an intrusion and information related to the computer.

2. The method of Claim 1, wherein the information related to the computer is based on whether the computer is a firewall for other computers in the computer system.

3. The method of Claim 1, wherein the information related to the computer is based on whether the computer is a server of information for other computers in the computer system.

4. The method of Claim 3, further comprising evaluating whether the computer serves as at least one of a webserver, an intranet application server, and a backend server.

5. The method of Claim 1, wherein the information related to the computer is based on whether the computer is protected by a firewall from a source of the intrusion.

6. The method of Claim 1, wherein the information related to the computer is based on memory utilization in the computer.

7. The method of Claim 1, wherein the information related to the computer is based on processor utilization in the computer.

8. The method of Claim 1, wherein the information related to the computer is based on information from other than the IDS manager that indicates an intrusion into the computer.

9. The method of Claim 1, wherein the information related to the computer is based on proximity of the computer to a source of the intrusion.

10. The method of Claim 1, further comprising downloading the local IDS policy from a network-accessible repository to the computer.

11. The method of Claim 1, wherein the local IDS policy comprises one or more response actions to be taken based on a notification from the network-accessible IDS manager of an intrusion.

12. The method of Claim 11, wherein the response action comprises terminating an application that is a target of an attack.

13. The method of Claim 11, wherein the response action comprises discarding information in a communication to the computer.

14. The method of Claim 11, wherein the response action comprises discontinuing communication with a source of the communication.

15. A computer system that responds to intrusions, the computer system comprising:

a plurality of computers, each comprising a local IDS policy;

an intrusion detection service (IDS) manager that is configured to generate for the computers at least one notification of an intrusion, and wherein each of the computers is configured to selectively respond to the notification based on the local IDS policy and information relating to the computer.

16. The computer system of Claim 15, wherein the IDS manager is configured to determine that an intrusion has occurred in the computer system, and is configured to generate a notification based on determining that an intrusion has occurred.

17. The computer system of Claim 16, wherein at least two of the computers respond differently to the same intrusion notification from the IDS manager.

18. The computer system of Claim 16, wherein at least one of the computers responds differently to the same intrusion notification repeated at least once over time.

19. The computer system of Claim 15, further comprising a plurality of sensors that are configured to sense events that may indicate one or more possible intrusions into the computer system, and that are configured to inform the IDS manager of the events, and wherein the IDS manager is configured to determine that an intrusion has occurred in the computer system by correlating the events from the sensors.

20. The computer system of Claim 15, wherein the computers are configured to download the local IDS policy from a policy repository.

21. The computer system of Claim 15, wherein at least one of the computers is configured to selectively respond to the notification based on the local IDS policy and whether the computer is a server of information for other computers in the computer system.

22. The computer system of Claim 15, wherein at least one of the computers is configured to selectively respond to the notification based on the local

IDS policy and whether the computer is protected by a firewall from a source of the intrusion.

23. The computer system of Claim 15, wherein at least one of the computers is configured to selectively respond to the notification based on the local IDS policy and based on at least one of memory utilization in the computer and processor utilization in the computer.

24. The computer system of Claim 15, wherein at least one of the computers is configured to selectively respond to the notification based on the local IDS policy and information relating to possible intrusions into the computer.

25. The computer system of Claim 15, wherein at least one of the computers is configured to selectively respond to the notification based on the local IDS policy and information relating to proximity of the computer to a source of the intrusion.

26. A computer program product for responding to an intrusion, the computer program product comprising program code embodied in a computer-readable storage medium, the computer program code comprising:

program code that is configured to selectively respond to at least one notification from a network-accessible intrusion detection service (IDS) manager of an intrusion based on local IDS policy and information relating to a computer.

27. The computer program product according to Claim 26, further comprising program code that is configured to download the local IDS policy from a network-accessible repository to the computer.

28. The computer program product according to Claim 26, further comprising program code that is configured to perform one or more response actions

based on the notification, the local IDS policy, and the information relating to the computer.

29. The computer program product according to Claim 26, further comprising program code that is configured to selectively respond to the notification based on whether the computer is a server of information for other computers in the computer system.

30. The computer program product according to Claim 26, further comprising program code that is configured to selectively respond to the notification based on at least one of whether the computer is protected by a firewall from a source of the intrusion and proximity of the computer to a source of the intrusion.

31. The computer program product according to Claim 26, further comprising program code that is configured to selectively respond to the notification based on at least one of memory utilization in the computer and processor utilization in the computer.